"Information Security Is Not Really My Job": Exploring Information Security Role Identity in End-Users

Obi Ogbanufe
Oklahoma State University
Obi.Ogbanufe@okstate.edu

Abstract

Given the significant role individuals play on the welfare of organizations' security, end users are encouraged to see themselves as part of the information security solution and are expected to perform certain end-user security roles. However, there is often a divide between the organization's expectations of the end-user's information security role and the end-user's functional role. We explore the concept of role identity in order to understand the factors that increase the importance ascribed to the information security end user role, which in turn affects performance and actions towards security behaviors. We develop a model that focuses on two issues: (1) factors that increase information security role identity (ISRI) and (2) consequents of ISRI, specific to security behaviors. A survey was used to explore the relationships in the model. Theoretical and practical implications of this research are presented.

1. Introduction

Given the recognition that employees play an important role in information security management [37,43], many organizations assign their employees a specific end-user role in the management of information security. End-users are encouraged to believe that their role is important in fulfilling the overall goal of information security (confidentiality, integrity, availability) [1], are encouraged to see themselves as part of the security management solution, and are expected to perform certain end-user security roles [18]. However, there is often a divide between the organization's expectations of the end-user's information security role and the end-user's business functions [1,31]. End-users are often caught between the divide. The divide becomes more pronounced when the individual's self-concept is tied to their business-functional role rather than the information security end-user role. For example, an individual in an accountant role or a salesperson role, might see themselves more as an accountant or salesperson, more so than as an information security end-user. The following is an exemplar account of an end-user caught between the role divide.

> *" We are measured by sale. Our salary depends on it, bonuses and stuff like that. Information security is definitively a second or third priority. If we have to use half an hour extra on information security per day – that simply doesn't function!"*
> [1:282].

The preceding account highlights how individuals could see themselves, their roles and the performance of such roles vis-a-vis their role in information security. How individuals see themselves affect how they act [9,14]. Users who see themselves as accountants, salespersons, or security administrators tend to act in a manner consistent with accountants, salespersons and security professionals, respectively. This is often referred to as role identity, which is described as a set of meanings and expectations defined by a social position in the social structure and that makes up a part of the individual's self-concept [10]. Role identity theorists have since recognized that individuals are often in varied roles that may span different groups, and therefore have multiple role identities [10,40]. Though these identities can complement each other, they can also compete with each other when the multiple identities are linked to "participations in different groups with potentially different agendas and expectations for members" [40:291]. Thus, resulting in conflicting expectations for the individual's behavior, as demonstrated in the above exemplar account of the salesperson who is also expected to perform in the role of information security.

Even though researchers and practitioners agree that the role of the end-user is important to information security, to date, there are few studies examining the link between the individual's role, specifically, their role

URI: https://hdl.handle.net/10125/64263
978-0-9981331-3-3

identity and security behaviors. Hence, the goal of this research is to examine information security behaviors through the mechanism of role identity.

The role identity literature has established that it is commonplace for individuals to have multiple role identities (e.g., mother, prosecutor), and that these identities are often ordered in a "hierarchy of salience" [40]. In this hierarchy of salience, one role identity (e.g., accountant) may be considered more important to the individual's self-concept. Further, the role identities on the higher rungs of the hierarchy that make up the individuals identity have been shown to have more influence on the individual's actions and performance [7,36]. Therefore, with respect to the current study, it seems that a key part of influencing the end user's information security behavior is to increase the importance of their information security role identity. That is, we explore factors that influence the information security role identity.

This leads us to seek answers to the following research questions: (1) w*hat factors affect information security role identity?* (2) *how does information security role identity affect secure behaviors*? The notion is that increasing the importance of information security role identity will in turn affect performance and actions towards security behaviors. We posit that role identity may hold the link that explains how end-users in organizations develop a sense of self relative to information security, and how such identity could influence security beahviors. We develop a model that focuses on two issues: (1) factors that increase information security role identity (ISRI) and (2) consequents of ISRI, specific to security behaviors. The proposed model, which integrates security literature [e.g., 1,17,18] and role identity theory [e.g., 8,40] provides a basis for identifying antecedents of ISRI and understanding its influence on security behaviors in the organization.

We anticipate that this research will contribute to research in two ways. First, that it bridges the functional versus information security role divide by introducing ISRI and examines how its strengthening affects security behaviors. By focusing on role identity, we address a gap in the information security literature concerning the relationship between role identity and security behaviors. Second, researchers note the relevance of the social aspect for security behaviors [12,30]. Researchers argue that because the decision to behave securely has consequences for both the individual and others in the organization, social factors are important in the formation of security-related behaviors [2]. The current study's application of the role identity stands to illuminate the mechanisms through which a social concept such as role identity creates a basis for security behaviors.

2. Theoretical Foundation

A role identity [5,40] is a self-concept, a *meaning* attributed to onself in relation to a particular role [6]. The meaning is verified through interacting with other people who respond to and treat the individual as a role player [6]. When others are not available or willing to verify or reaffirm this identity, the role identity may dwindle [39]. Thus, confirming the dynamics between how "self-concepts and social environments shape and sustain each other" [36:168].

According to Stryker and Burke [40], role identity represents a twofold concept. On the one hand, role is external and suggests a connection to a social position within a social structure. Whereas, identity is internal, suggesting that the ascribed meanings and expectations are internal in its formation [40]. When the individual's identity is closely aligned with their role, they tend to behave in line with the role identity, which in turn verifies their identity [8]. Researchers suggest that an important factor affecting the enactment of role identities is the way they are structured hierarchically [10,26]. Also referred to as role identity salience, it is the idea of giving a particular role identity more importance relative to other role identities one may have [8,10]. For the accountant, the accountant role identity may be the central aspect of their self-concept. Thus, dominating other role-identities (such as information security end-user role) and affecting their behaviors. As a result, the employee's primary role, which is the basis of their self-concept takes precedence, while the ISRI may take a back seat in the employee's daily task performance. Hence, it is important to explore ways to increase the ISRI in the end-user.

The literature suggests that an individual's sense of role identity is derived from feedback about the self from social relations and associated self-views [34]. Specifically, role identity can also be influenced by social context variables such as (1) normative expectations of others [14], (2) social support the individuals receives in the role [8,10], (3) self-views [14,42], and (4) the surrounding environment [33]. We elaborate on these below.

2.1. Antecedents of Information Security Role Identity

2.1.1. Normative expectation of others. Normative expectation is the degree to which significant others identify the end-user with the information security role

[14]. Normative expectations of others can influence how individuals see themselves. When individuals see themselves through the expectations of others, it can influence the individual's behavior. Due to norms from significant others, individuals may perform certain roles expected of them [44]. There is ample support in information security research suggesting that the expectations of supervisors and peers influence employee security behaviors [17]. Others note that specific significant others such as chief security officers and security managers might provoke some behavioral changes from their end-users to observe security procedures [20]. Managers' expectations of information security can influence information security behaviors [18].

These expectations can be expressed through information security policies that describe actions that end-users should follow. Since identity is usually formed, verified, and strengthened through interactions with others, we posit that the expectations of managers will increase ISRI in the end user. That is, role identity theorists suggest that individuals that perceive that significant others expect them to exhibit proper information security behaviors will likely define themselves as information security end-users. Identity research has found significant relationships between normative expectations and role identity [e.g., 7,14]. We hypothesize:

H1: Others information security expectations positively influences ISRI

2.1.2. Social Support. Generally, social support refers to the amount of social support one receives in the role identity [26]. There is a general understanding that when individuals receive support in an activity, it increases the likelihood that the individual will exert more effort in the task or role [46,47]. Social support and interacting with others in specific role activities has been studied in online health [27] and can represent an individual's "social need as well as their active participation" in specific role activities with others [48:644]. In information security, social support could be achieved through involving end-users in security, education, training and awareness (SETA) campaigns and encouraging end-user participation in information security management [1,37].

Social support through participating in workshops also allow end-users to learn more about security threats, threat avoidance techniques, and appropriate behavioral responses. Participating in SETA and workshops gives the end-user a sense that they are being supported and provided with the right tools. End-users can share their frustrations about the security landscape and receive information that can help them behave securely in their day-to-day activities. For example, involving users and encouraging their continuous participation in the organization's security risk management program aligns information security initiatives with business objectives [37], thus increasing the importance attributed to the information security role identity. When end-users believe that they receive adequate support from the organization in their information security end-user role, it increases ISRI. We hypothesize:

H2: Perceptions of social support in information security positively influences ISRI

2.1.3. Self-views. Self-views refer to thoughts and feelings about oneself [42]. We define self-views as the individual's views of their own security behavior [14]. Self-verification theory [3,41,42] suggests that individuals' self-views help them make sense of the world and how others may perceive them. For example, an individual's belief that s/he is a mother/father provides them with a set of beliefs about their role in the larger society. Similarly, an employee's belief that s/he complies with information security policy could provide them with notions of their information security role in the organization.

Generating self-meaning though role identity comes from a sense making process that reconciles inputs from others and inputs from the self in order to validate and verify the identity [34]. When an individual interprets their previous role activities, role identity can develop over time as a result [15]. This relationship is consistent with the social psychology theory, which suggests that past behavior generates a related self-concept. Also, because self-views give people a strong sense of consistency, they are often motivated to maintain such views [41]. Hence, past security behavior, as seen by the self, should predict future secure behaviors as the individual tries to make his/her identity consistent with past role-related behaviors [14]. Previous studies have found support for the relationship between self-views of a behavior and a related role identity. For example, Farmer et al. [14] found that self-views of creative behaviors influenced creative role identity. We hypothesize:

H3: Self-views of information security behaviors positively influences ISRI

2.2 Information Security Role Identity and Secure Behaviors

The role identity literature suggests that role identity leads to related role behaviors [5,10,26]. This is mainly because the performance of the relevant roles satisfies an important need for self-verification [25]. Although individuals may have multiple role identities in the organization, an increase in the importance of certain

role identities tend to affect the behaviors enacted [10,26]. There is strong evidence showing the relationship between specific role identities and the corresponding role performances. For example, a creative role identity has been found to influence creative behaviors [14]. Also, blood donation [10] and volunteer role identities [7] strongly influenced blood donation and volunteering behaviors, respectively.

Previous research suggests that because of the important role that users play in information security management, researchers should examine the mechanisms through which security behaviors are generated [1,32]. Hence, we suggest that a mechanism through which this behavior manifests is role identity. Building on the role identity literature that explicitly suggests that role identity affects behavior [7,10,14,22], we posit that increases ISRI will affect security behaviors. We hypothesize:

H4: ISRI positively influences security behaviors

There is demonstrable evidence that suggests that an important antecedent to security behaviors is threat perception [21,45]. Perceived threat is defined as the extent to which individuals perceive the security threat as harmful [23]. The central theme of the behavioral security literature is that when individuals perceive a security threat (e.g., phishing email, malware, stolen password etc.), they will use a safeguarding measure or behave securely (e.g., delete suspicious email, download only secure software) in order to prevent, avoid, or reduce the impact of the threat [e.g., 11,23]. We hypothesize:

H5: Perceived security threat positively influences security behaviors

In the previous section, we used the literature to establish that role identity (i.e., ISRI) affects role behaviors and that cybersecurity threat perceptions affect behaviors. In order to more fully understand the conditions under which threat perception and ISRI are related to secure behaviors [24], we consider threat perception as a moderator. Threat perception is likely to be useful in explaining the conditions under which ISRI exerts the most or least influence on secure behaviors.

In an organization with changing environments, individuals usually seek to reduce uncertainties by identifying with certain roles [3]. Research on identities indicate that environmental changes increase the chance that individuals will reevaluate identities, suggesting that perceptions based on external forces can sometimes lead to alterations to an identity [33:436]. Hence, it is possible that when individuals are exposed to changes or damages to the organization resulting from cybersecurity threats, it may affect how their identity with the information security role influences their behavior. In other words, substantive changes about security breaches affecting one's organization or industry, such as news about security lapses, phishing attacks involving end-users, may prompt individuals to develop new interpretations of their information security role identity with respect to their security behaviors. We hypothesize:

H6: Perceived security threat moderates the positive relationship between ISRI and security behaviors

The proposed research model is shown in Figure 1 below

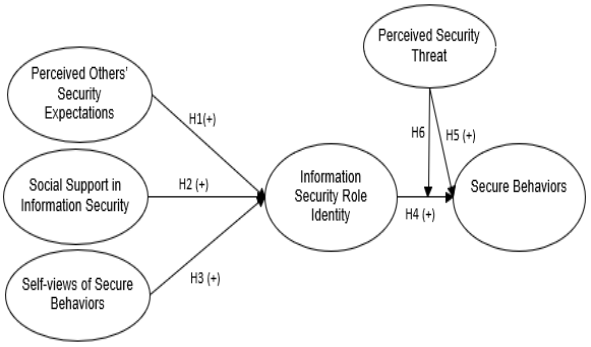

Figure 1: Research Model

3. Research Method

3.1 Measurement

We examine the proposed research model and hypotheses using a survey. Previously validated measures are adapted to the context of the study. The measures for perceived others expectation were adapted from Herath and Rao [16] and Farmer et al. [14]. We operationalized social support with user participation. The measures for perceived user participation were adapted from Hsu et al. [18] and Spears and Barki [37]. The measures for perceived security threat and self-views were adapted from Liang and Xue [23] and Farmer et al. [14], respectively. Role identity was adapted from Callero [7,8], and contextualized for the information security end user role. Measures for secure behaviors were adapted from Posey et al. [30].

Following Podsakoff et al., [29], we used standard procedures to minimize common-method variance. Attention filters were presented to ensure that respondents carefully read the items. To minimize social desirability bias, respondents' anonymity was assured, they were also assured that there were no right or wrong answers. In addition, measures were assessed using a

seven-point Likert and semantic differential scales that were anchored by 1 = strongly disagree and 7 = strongly agree.

3.2. Sample

We recruited participants from Amazon Mechanical Turk (MTurk). MTurk represents a large diversity of participants and the data is considered as reliable as those collected from other methods [4,19]. Following Steelman et al. [38], we required all participants to be within the United States. We also required participants to be employed full time (i.e., at least work 35 hours per week). Out of 161 participants who attempted the survey, 129 completed the survey, giving us a completion rate of about 80 percent. The sample consisted of 129 individuals from various industries and functional roles within the United States. The respondents demographics include, males 48.4%, females 50.8%, other 0.8%. 52% of respondents have been in their current role for 1 to 5 years, followed by 27% occupying their role for 6 to 10 years. The functional roles include IT (23%), customer service (16%), operations (15%) management (12%).

4. Data Analysis and Results

4.1. Measurement Model

We used SmartPLS 3.0 [35]. To investigate the adequacy of the measures, reliability, discriminant validity and convergent validity were examined. Reliability was examined based on Cronbach's Alpha (CA). A scale is reliable if CA is greater than 0.70 [28]. Construct validity for the scale items were assessed, including AVE (average variance extracted). All the AVE estimates were higher than 0.5, and the square root of all AVEs were higher than the inter-construct correlations. These results provide evidence of acceptable internal consistency, convergent and discriminant validity, and construct validity for the scale items used in this study. Tables 1 presents evidence of reliability and construct validity, as well as the correlations between constructs. We examined multi-collinearity using variance inflation factor (VIF) statistics, and the highest VIF is 1.83, which is below the VIF threshold value of 3.3 [13]. Hence, desired low multi-collinearity was achieved.

	CA	AVE	1	2	3	4	5	6
(1)	0.94	0.73	**0.86**					
(2)	0.81	0.63	0.43	**0.79**				
(3)	0.92	0.81	0.64	0.61	**0.90**			
(4)	0.84	0.68	0.19	0.59	0.47	**0.83**		
(5)	0.87	0.71	0.28	0.60	0.58	0.70	**0.84**	
(6)	0.87	0.71	0.29	0.46	0.42	0.56	0.64	**0.84**

(1) SOCS: Social support, (2) OEXP: Other's Expectations, (3) ISRI: information security role identity, (4) SVW: Self-views, (5) BEH: Secure Behaviors, (6) THR: Perceived Threat

Table 4: Correlations

Harman's single factor test evaluates whether one factor is responsible for the majority of covariance among the variables by performing an unrotated factor analysis of the factors [29]. Six factors emerge with the largest factor explaining 40% of the variance. Since this is less than half, our data passes the Harman's single factor test.

4.2. Structural Model

Following the determination that the measurement model was sound, we then evaluated the strength of relationships between the model's constructs indicated by path coefficients and the predictive power of the model based on R-square values. As hypothesized, all relationships are significant at 0.01 level. 57.9% of information security role identity is explained by perceived others' expectations, self-views of security behaviors, and social support. Information security role identity and perceived threat are significant in their relationships to secure behaviors. We also found that perceived threat significantly moderates the relationship between role identity and secure behaviors. The model explains 58% of the variance in the dependent variable, secure behaviors. A summary of the results of the structural model are presented in Table 2 and explained in the following discussion section.

Hypothesis	Est.	SD	TStats	Pvalue
SOCS → ISRI	0.482	0.067	7.208	0.000
SVW → ISRI	0.218	0.085	2.574	0.010
OEXP → ISRI	0.274	0.084	3.277	0.001
ISRI → BEHV	0.404	0.076	5.284	0.000
THR → BEHV	0.436	0.055	7.929	0.000
THR * ISRI → BEHV	-0.220	0.047	4.629	0.000

SOCS: Social support, SVW: Self-views, OEXP: Other's expectations, THR: Perceived threat, ISRI: information security role identity. SD: Standard deviation

Table 2. Structural Model Results

5. Discussion

The cybersecurity literature recognizes that employees play an important role in security management [37,43] and that there is an expectation for employees to perform certain end-user security roles [18]. Also, research in role identity [10,40] has since recognized that a sense of identity in a particular role has a strong influence on related role behaviors. However, there are few studies examining the link between the individual's role, specifically, their role identity and security behaviors. Hence, the goal of this research is to examine information security behaviors through the mechanism of role identity. We did so by drawing from the cybersecurity literature and role identity literature to explain how social aspects influence the information security role identity, and in turn secure behaviors.

There are a few findings from this study. First, by integrating role identity in information security research, we highlight and demonstrate the importance of role identity in advancing and motivating information security behaviors. In addition, the relatively high R-squares achieved for the dependent variables (comparable to the results of prior security behaviors research) confirm the appropriateness of examining the influence of the role identity and its impact on secure behaviors.

Second, the importance of self-views is also highlighted in this study. The positive and significant relationship between an individual's self-views and their role identity demonstrates that individuals that hold positive self-views of themselves performing secure behaviors will develop information security role identities.

Third, we also find that social support by way of participating in information security activities in the organization positively influences information security role identity. This finding confirms that engaging users in security activities in ways that make them feel supported can engender information security role identity. Furthermore, we found significant positive effects between perceived expectations of others and information security role identity. This result is consistent with role identity research that suggests that when an individual perceives that coworkers, managers, and IT support staff expect them to behave securely, their role identities as information security end-users increases.

Finally, even though threat perception is recognized as a key factor for motivating secure behaviors, individuals may still lack the motivation to behave securely. This is because individuals may not see information security as important or important to their self-concept. Hence, by examining the interaction of information security role identity and security threat perception, we demonstrate that these two factors interact to influence secure behaviors. We found that threat perception significantly weakens the relationship between role identity and secure behaviors. The result demonstrates the notion that external threats and forces can potentially change the individual's identity interpretation [33] and behaviors. For example, an individual's political/religious affiliation role identity may influence how much time and money they give to the affiliation (i.e., behavior). However, when the individual perceives that the political/religious organization is threatened by external forces (i.e., threat perception), this may reduce how much money and time the individual gives, with respect to their political/religious role identity.

5.1. Research Implications

We contribute to research in two ways. First, we attempt to bridge the functional versus information security role divide by introducing information security role identity and examine how its strengthening affects security behaviors. By focusing on role identity, we address a gap in the information security literature concerning the relationship between role identity and security behaviors. This research identifies factors that increase the importance of the information security role identity, and in turn secure behaviors.

Second, researchers note the relevance of the social aspect for security behaviors [e.g., 12,30]. Researchers argue that because the decision to behave securely has consequences for both the individual and others in the organization, social factors are important in the formation of security-related behaviors [2]. The current study's application of the role identity stands to illuminate the mechanisms through which a social concept such as role identity creates a basis for security behaviors.

Overall, the results suggest that researchers pay more attention to the influence of social forces on information security role identity, particularly factors involving norms and expectations in the workplace.

5.2. Practical Implications

As more organizations increasingly provide employees with access to corporate secrets, sensitive systems, and proprietary information, the role of the end user in protecting organizations' resources becomes more important. The results show that information security role identity is shaped by self-views and social relations (others' expectation, social support). Hence, organizations and security managers looking to enhance and shape their employees information security role identity, which in turn shapes secure behaviors, could

do so by finding creative ways to express security behavior expectations. Perhaps, these expectations can be expressed through emails, posters in common areas, or during team meetings. In addition, since this research implies that social support increases role identity, security managers could engage users by allowing them to meaningfully participate in information security activities if they are to develop information security role identities.

5.3. Limitations and Future Research

This study has limitations that create opportunities for future research. First, as an initial investigation of the social factors affecting information security role identity, only a few variables were identified in this study. A future study would include more factors that might further increase information security role identity. Second, although common method bias was assessed, and we found little evidence that it accounted for our results. Hence, future research should use more procedures to minimize common-method variance. Since this research surveyed only those in the U.S., future research could survey respondents from other countries to explore the impact of culture on information security role identity.

5.4. Conclusion

In conclusion, this study explores the concept of role identity in order to understand the factors that increase the importance ascribed to the information security end user role, which in turn affects performance and actions towards security behaviors. This study addresses a gap in the information security literature concerning the relationship between role identity and security behaviors and suggests that more attention be given to the influence of social factors on information security behaviors.

6. References

[1] Albrechtsen, E. A qualitative study of users ' view on information security. *Computers and Security*, *26*, 0167 (2007), 276–289.

[2] Anderson, C. and Agarwal, R. Practicing Safe Computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quartely*, *34*, 3 (2010), 613–643.

[3] Ashforth, B.E., Harrison, S.H., and Corley, K.G. Identification in Organizations: An Examination of Four Fundamental Questions. *Journal of Management*, *34*, 3 (2008), 325–374.

[4] Buhrmester, M. and Kwang, T. Amazon's Mechanical Turk a new source of inexpensive, yet high-quality, data? *Perspectives on Psychological Science*, *6*, 1 (2011), 3–5.

[5] Burke, P. and Reitzes, D. The Link Between Identity and Role Performance. *Social Psychology Quarterly*, *44*, 2 (1981), 83–92.

[6] Burke, P. and Tully, J. The Measurement of Role Identity. *Social Forces*, *55*, 4 (1977), 881–897.

[7] Callero, P., Howard, J., and Piliavin, J. Helping behavior as role behavior: Disclosing social structure and history in the analysis of prosocial action. *Social Psychology Quarterly*, (1987), 247–256.

[8] Callero, P.L. Role-Identity Salience. *Social Psychology Quarterly*, *48*, 3 (1985), 203–215.

[9] Carter, M. and Grover, V. Me, Myself, and I(T): Conceptualizing Information Technology Identity and its Implications. *MIS Quarterly*, *39*, 4 (2015), 931–957.

[10] Charng, H.-W.H., Piliavin, J.A., and Callero, P.L. Role identity and reasoned action in the prediction of repeated behavior. *Social Psychology Quarterly*, *51*, 4 (1988), 303–317.

[11] Chen, Y. and Zahedi, F.M. Individuals ' Internet Security Perceptions and Behaviors : Polycontextual Contrasts Between the Unites States and China. *MIS Ouarterly*, *40*, 1 (2016), 205–222.

[12] Dhillon, G. and Backhouse, J. Current directions in IS security research : towards socio-organizational perspectives. *Information Systems Journal*, *11*, 1 (2001), 127–153.

[13] Diamantopoulos, A. The error term in formative measurement models: interpretation and modeling implications. *Journal of Modelling in Management*, *1*, 1 (2006), 7–17.

[14] Farmer, S.M., Tierney, P., and Kung-Mcintyre, K. Employee Creativity in Taiwan : An Application of Role Identity Theory. *Academy of Management Journal*, *46*, 5 (2003), 618–630.

[15] Grube, J.A. and Piliavin, J.A. Role Identity, Organizational Experiences, and Volunteer Performance. *Personality and Social Psychology Bulletin*, *26*, 9 (November 2000), 1108–1119.

[16] Herath, T. and Rao, H.R. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*, 2 (2009), 106–125.

[17] Herath, T. and Rao, R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*, 2 (2009), 154–165.

[18] Hsu, J.S.-C., Shih, S.-P., Wen Hung, Y., and Lowry, P.B. The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness. *Information Systems Research*, *26*, 2 (2015), 0–19.

[19] Jenkins, J.L., Anderson, B.B., Vance, A., Kirwan, C.B., and Eargle, D. More Harm Than Good? How Messages That Interrupt Can Make Us Vulnerable. *Information Systems Research*, *27*, 4 (2016).

[20] Johnston, A.C. and Warkentin, M. Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, *34*, 3 (2010), 549-A4.

[21] Johnston, A.C., Warkentin, M., and Siponen, M. An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric. *MIS Quarterly*, *39*, 1 (2015), 113-A7.

[22] Lee, Y., Lee, J., and Lee, Z. Social influence on technology acceptance behavior: Self-Identity Theory perspective. *Database for Advances in Information Systems*, *37*, 2 & 3 (2006), 60–75.

[23] Liang, H. and Xue, Y. Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information*, *11*, 7 (2010), 394–413.

[24] MacKinnon, D.P. and Luecken, L.J. How and for whom? Mediation and moderation in health psychology. *Health Psychology*, *27*, 2 (2008), S99–S100.

[25] Markus, H. and Wurf, E. The Dynamic Self-Concept: A Social Psychological Perspective. *Annual Review of Psychology*, *38*, 1 (January 1987), 299–337.

[26] McCall, G.J. and Simmons, J.L. *Identities and Interactions*. Free Press, New York, 1978.

[27] Mein Goh, J., Gao, G., and Agarwal, R. The Creation of Social Value: Can an Online Health Community Reduce Rural-Urban Health Disparities? *MIS Quarterly*, *40*, 1 (2016), 247–263.

[28] Nunnally, J.C. and Bernstein, I.H. Pyschometric Theory. In *A catastrophe model for developing service satisfaction strategies. Journal of Marketing*. *56*. McGraw-Hill, New York, 1994, pp. 83–95.

[29] Podsakoff, P.M., MacKenzie, S.B., Lee, J.-Y., and Podsakoff, N.P. Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of applied psychology*, *88*, 5 (2003), 879.

[30] Posey, C., Roberts, T.L., Lowry, P.B., Bennett, R.J., and Courtney, J.F. Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors. *MIS Quarterly*, *37*, 4 (2013), 1189–1210.

[31] Posey, C., Roberts, T.L., Lowry, P.B., and Hightower, R.T. Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management*, *51*, 5 (2014), 551–567.

[32] Rasmussen, J. Risk management in a dynamic society: A modelling problem. *Safety Science*, *27*, 2–3 (1997), 183–213.

[33] Ravasi, D. and Schultz, M. Responding to Organizational Identity Threats : Exploring the Role of Organizational Culture. *Academy of Management Journal*, *49*, 3 (2006), 433–458.

[34] Riley, A. and Burke, P. Identities and self-verification in the small group. *Social Psychology Quarterly*, *58*, 2 (1995), 61–73.

[35] Ringle, C.M., Wende, S., and Becker, J.-M. SmartPLS 3.0. 2015. http://www.smartpls.com.

[36] Smith-Lovin, L. Self, Identity, and Interaction in an Ecology of Identities. In P. Burke, T. Owens, R. Serpe and P. Thoits, eds., *Advances in Identity Theory and Research*. Springer US, Boston, MA, 2003, pp. 167–178.

[37] Spears, J.L. and Barki, H. User participation in information systems security risk management. *MIS Quarterly*, *34*, 3 (2010), 503-A5.

[38] Steelman, Z.R., Hammer, B.I., and Limayem, M. Data Collection in the Digital Age: Innovative Alternatives to Student Samples. *MIS Quarterly*, *38*, 2 (2014), 355–378.

[39] Stets, J.E. and Burke, P. Identity theory and social identity theory. *Social Psychology Quarterly*, (2000), 224–237.

[40] Stryker, S. and Burke, P. The past, present, and future of an identity theory. *Social Psychology Quarterly*, (2000), 284–297.

[41] Swann, W.B. Self-verification theory. In L. Paul, A. Kruglanski and T. Higgings, eds., *Handbook of Theories of Social psychology*. 2011, pp. 23–42.

[42] Swann, W.B., Polzer, J.T., Seyle, D.C., Ko, S.J., Nn, W.B.S.W., and Diamond, J. Verification Value in Diversity : Finding of Personal and Social Self-Views in Diverse Groups. *Academy of Management Review*, *29*, 1 (2004), 9–27.

[43] Vance, A., Benjamin Lowry, P., and Eggett, D. Increasing Accountability Through User-Interface Design Artifacts: A New Approach To Addressing the Problem of Access-Policy Violations. *MIS Quarterly*, *39*, 2 (2015), 345–366.

[44] Venkatesh, V., Sykes, T.A., and Venkatraman, S. Understanding e-Government portal use in rural India: role of demographic and personality characteristics. *Information Systems Journal*, *24*, 3 (May 2014), 249–269.

[45] Wang, J., Xiao, N., and Rao, H.R. An exploration of risk characteristics of information security threats and related public information search behavior. *Information Systems Research*, *26*, 3 (2015), 619–633.

[46] Woo Yoo, C. and Raghav Rao, H. Collective Security Efficacy and Group Security Compliance. In *Thirty Fifth International Conference on Information Systems*. AIS, Auckland, 2014, pp. 11.

[47] Wood, R. and Bandura, A. Social Cognitive Theory of Organizational Management. *Academy of Management Review*, *14*, 3 (July 1989), 361–384.

[48] Yan, Z., Wang, T., Chen, Y., and Zhang, H. Knowledge sharing in online health communities: A social exchange theory perspective. *Information & Management*, *53*, 5 (2016), 643–653.